(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. Juli 2002 (25.07.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/057905 A1

(51) Internationale Patentklassifikation[7]: G06F 9/30

(21) Internationales Aktenzeichen: PCT/DE02/00110

(22) Internationales Anmeldedatum:
16. Januar 2002 (16.01.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 01 956.4 17. Januar 2001 (17.01.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HARTLIEB, Heimo** [AT/AT]; Rudersdorferstr. 164, A-8055 Graz (AT). **SEDLAK, Holger** [DE/DE]; Neumünster 10a, 85658 Egmating (DE). **KLUG, Franz** [AT/DE]; Ottobrunner Str. 17, 81737 München (DE).

(74) Anwalt: **EPPING, HERMANN & FISCHER**; Ridlerstr. 55, 80339 München (DE).

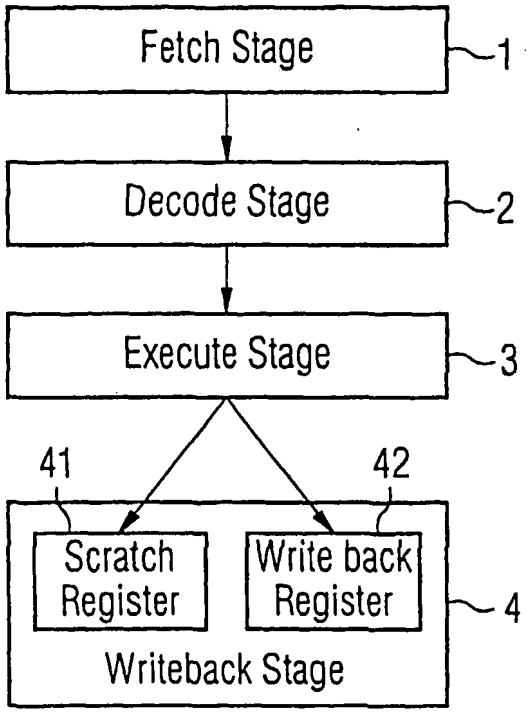
(81) Bestimmungsstaaten *(national)*: BR, CA, CN, IL, IN, JP, KR, MX, RU, UA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR INCREASING THE SECURITY OF A CPU

(54) Bezeichnung: VERFAHREN ZUR ERHÖHUNG DER SICHERHEIT EINER CPU



(57) Abstract: The invention relates to a method for increasing the security of a CPU, which is characterized by using a pipeline that comprises a fetch stage (1), a decode stage (2), an execute stage (3) and a writeback stage (4), said writeback stage having at least one register (41) and at least one register (42). When the register (41) is used, the status of the CPU remains unchanged, while when the register (42) is used, the status of the CPU is changed. The inventive method is further characterized in that in the decode stage at least one randomly chosen code sequence is inserted as the dummy code sequence or filler, thereby making an attack by DPA more difficult.

(57) Zusammenfassung: Bei dem Verfahren wird eine Pipeline bestehend aus einer Ladestufe (1), einer Decodierstufe (2), einer Ausführungsstufe (3) und einer Rückspeicherstufe (4) verwendet. Die Rückspeicherstufe besitzt mindestens ein Register (41), bei dessen Benutzung keine Zustandsänderung der CPU erfolgt, und mindestens ein Register (42), bei dessen Benutzung eine Zustandsänderung der CPU erfolgt. Erfindungsgemäß wird in der Decodierstufe mindestens eine zufällig ausgewählte Codesequenz als Platzhalter-Code oder Füllsel eingefügt, womit ein Angriff durch DPA erschwert wird.

WO 02/057905 A1

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zur Erhöhung der Sicherheit einer CPU

Die vorliegende Erfindung betrifft ein Verfahren zur Verbesserung der Sicherheit einer CPU.

Differential Power Analysis (DPA) ist ein bekanntes Angriffsszenario für Sicherheits-CPUs. Bei einem solchen Angriff wird eine Folge von Programmbefehlen und deren Auswirkungen in der CPU mittels statistischer Auswertungen der Kennlinien des Stromverbrauchs ermittelt. Aus diesen Auswertungen lassen sich detaillierte Rückschlüsse über das ausgeführte Programm gewinnen.

In der DE 199 36 939 A1 und der WO 00/50977 sind Verfahren beschrieben, mit denen insbesondere für eine Anwendung bei Chipkarten eine DPA dadurch erschwert wird, dass nur zur Täuschung vorgesehene Rechenoperationen beziehungsweise Programmschritte durchgeführt werden, die nach einer zufälligen Auswahl in die Programmabläufe eingeschleust werden.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren zur Erhöhung der Sicherheit einer CPU anzugeben.

Diese Aufgabe wird mit dem Verfahren mit den Merkmalen des Anspruches 1 gelöst. Ausgestaltungen ergeben sich aus den abhängigen Ansprüchen.

Bei dem erfindungsgemäßen Verfahren wird eine als Pipeline aufgebaute CPU mit mindestens einer Decodierstufe und einer Rückspeicherstufe verwendet, die typisch eine Ladestufe (Fetch Stage), eine Decodierstufe (Decode Stage), eine Ausführungsstufe (Execute Stage) und eine Rückspeicherstufe (Writeback Stage) umfasst. Die Rückspeicherstufe besitzt mindestens ein Register, bei dessen Benutzung keine Zustandsänderung der CPU erfolgt, und mindestens ein Register, bei des-

sen Benutzung eine Zustandsänderung der CPU erfolgt. Erfindungsgemäß wird in der Decodierstufe mindestens eine zufällig ausgewählte Codesequenz als Platzhalter-Code oder Füllsel eingefügt. Dieses Verfahren ist im Prinzip für beliebige Pipelines anwendbar, die insbesondere zusätzlich zu den als Beispiel angegebenen Stufen über weitere Stufen verfügen können, und wird anhand der beigefügten Figuren näher erläutert.

Die Figur 1 zeigt ein Diagramm der beschriebenen Pipeline. Die Figur 2 zeigt ein Schema für das Vorgehen beim Einfügen der Codesequenzen.

In der Figur 1 ist ein Ablaufdiagramm dargestellt, das den Programmablauf von der Ladestufe 1 über die Decodierstufe 2 in die Ausführungsstufe 3 und von dort in die Rückspeicherstufe 4 einer als Beispiel dargestellten Pipeline zeigt. Die Rückspeicherstufe 4 besitzt hier mindestens ein erstes Register 41 als Scratch-Register und ein zweites Register 42 als Writeback-Register. Das Scratch-Register ist ein Register, bei dessen Benutzung keine Zustandsänderung der CPU erfolgt, während bei der Benutzung des Writeback-Registers eine Zustandsänderung der CPU erfolgt. Zur Erhöhung der Sicherheit der CPU wird von der Decodierstufe 2 eine Codesequenz, und zwar im Prinzip eine beliebige Codesequenz, in den Programmcode, der in der Pipeline übermittelt wird, eingeschleust. Es ist auch möglich, an mehreren Stellen des Programmcodes eine jeweilige zusätzliche Codesequenz als Platzhalter oder Füllsel (dummy code sequence) einzufügen. Das ist in der Figur 2 im Schema dargestellt.

Die Figur 2 zeigt im Schema eine Codesequenz 5 eines beliebigen Programms. In dieser Codesequenz 5 werden zufällig ausgewählte Codesequenzen 6 (Dummy-Sequenzen) an verschiedenen vorgegebenen oder ebenfalls zufällig ausgewählten Stellen eingefügt, so dass sich die erweiterte Codesequenz 50 ergibt. Die eingefügten Codesequenzen können zum Beispiel aus einem Speicher, insbesondere aus einem ROM, ausgelesen werden.

Die einzelnen Befehle zum Einfügen von Codesequenz können beispielsweise durch den Abruf von Adressen, die ein Zufallszahlengenerator erzeugt, generiert werden. Die einzufügenden Codesequenzen werden aus dem Speicher ausgelesen und an den Decoder in zufälliger Länge und Reihenfolge übermittelt. Der Decoder schleust den Code dieser Dummy-Codesequenzen in den laufenden Programmcode (Codestream) ein. Auch die Adressen, an denen der zufällig ausgewählte Code in den Programmcode eingeschleust wird, können mit einer an sich bekannten Zufallsmethode ermittelt werden.

Durch die zufallsbedingt eingefügte Codesequenz oder die mehreren zufällig ausgewählten und eingefügten Codesequenzen, die nur als Platzhalter oder Füllsel fungieren, wird keine Zustandsänderung der CPU hervorgerufen. Ein wesentlicher Vorteil dieses Verfahrens ist dabei, dass sich die Ausführungszeit des eigentlichen Programmcodes bei jedem Durchlauf desselben Programms gegenüber den vorhergehenden Durchläufen beliebig verändern lässt und dadurch ein Angriffsversuch, welchem statistische Auswertungen zugrunde liegen (wie zum Beispiel der eingangs erwähnten DPA), wesentlich erschwert ist.

Bezugszeichenliste

1 Ladestufe
2 Decodierstufe
3 Ausführungsstufe
4 Rückspeicherstufe
5 Codesequenz
6 zufällig ausgewählte Codesequenz
41 erstes Register (Scratch-Register)
42 zweites Register (Writeback-Register)
50 erweiterte Codesequenz

Patentansprüche

1. Verfahren zur Erhöhung der Sicherheit einer CPU, bei dem eine Pipeline aus mindestens einer Decodierstufe (2) und einer Rückspeicherstufe (4) mit mindestens einem ersten Register (41), bei dessen Benutzung keine Zustandsänderung der CPU erfolgt, und mit mindestens einem zweiten Register (42), bei dessen Benutzung eine Zustandsänderung der CPU erfolgt, eingesetzt wird,
d a d u r c h g e k e n n z e i c h n e t, dass
in der Decodierstufe (2) mindestens eine zufällig ausgewählte Codesequenz als Platzhalter-Code oder Füllsel eingefügt wird, die keine Zustandsänderung der CPU bewirkt, und
zusätzliche Mittel vorhanden sind, die dafür vorgesehen sind, sicherzustellen, dass bei jedem Durchlauf eines bestimmten Programms eine als Platzhalter-Code oder Füllsel verwendete und zufällig ausgewählte Codesequenz derart ausgewählt wird, dass eine jeweils von vorhergehenden Programmdurchläufen verschiedene Ausführungsdauer des Programms bewirkt wird.

2. Verfahren nach Anspruch 1, bei dem
eine oder mehrere zufällig ausgewählte Codesequenzen aus einem Speicher anhand einer bzw. mehrerer zufällig ermittelter Speicheradressen ausgelesen werden.

3. Verfahren nach Anspruch 2, bei dem
als Speicher ein ROM verwendet wird.

1/1

FIG 1

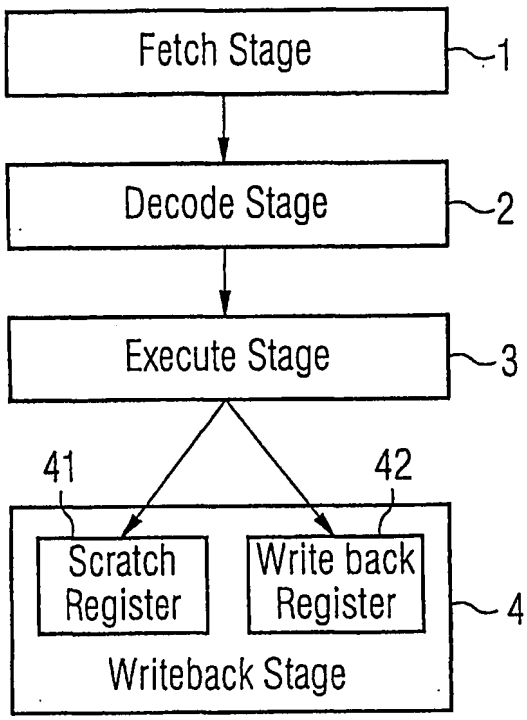
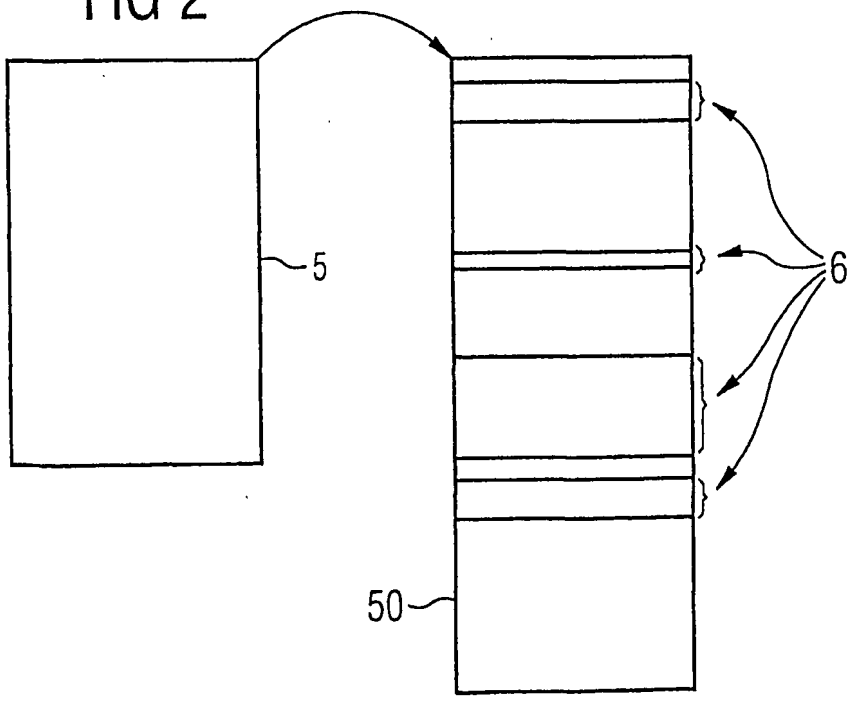

Fetch Stage
1
Decode Stage
2
Execute Stage
3
41
42
Scratch Register
Write back Register
4
Writeback Stage

FIG 2


5
6
50

INTERNATIONAL SEARCH REPORT

Int al Application No
PCT/DE 02/00110

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 50977 A (ROMAIN FABRICE ;ST MICROELECTRONICS SA (FR)) 31 August 2000 (2000-08-31) cited in the application abstract page 1, line 9-22 page 2, line 25 -page 3, line 9 page 4, line 4 - line 27 page 5, line 6 - line 15 page 5, line 31 -page 6, line 3 claim 1 ---	1-3
A	US 6 108 797 A (WU MENG-TSANG ET AL) 22 August 2000 (2000-08-22) abstract figure 3 claim 1 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 2002	27/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sadoune, M-M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In al Application No
PCT/DE 02/00110

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 199 36 939 A (PHILIPS CORP INTELLECTUAL PTY) 6 April 2000 (2000-04-06) abstract claim 1 figure 1	1
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 13, 30 November 1999 (1999-11-30) & JP 11 232092 A (NIPPON TELEGR &TELEPH CORP <NTT>), 27 August 1999 (1999-08-27) abstract	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Application No
PCT/DE 02/00110

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0050977 A	31-08-2000	FR 2790347 A1	01-09-2000
		EP 1163562 A1	19-12-2001
		WO 0050977 A1	31-08-2000
US 6108797 A	22-08-2000	TW 408264 B	11-10-2000
DE 19936939 A	06-04-2000	DE 19936939 A1	06-04-2000
		WO 0019386 A1	06-04-2000
		EP 1046142 A1	25-10-2000
JP 11232092 A	27-08-1999	NONE	

INTERNATIONALER RECHERCHENBERICHT

Int nales Aktenzeichen
PCT/DE 02/00110

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F9/30

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 00 50977 A (ROMAIN FABRICE ;ST MICROELECTRONICS SA (FR)) 31. August 2000 (2000-08-31) in der Anmeldung erwähnt Zusammenfassung Seite 1, Zeile 9-22 Seite 2, Zeile 25 -Seite 3, Zeile 9 Seite 4, Zeile 4 - Zeile 27 Seite 5, Zeile 6 - Zeile 15 Seite 5, Zeile 31 -Seite 6, Zeile 3 Anspruch 1 ---	1-3
A	US 6 108 797 A (WU MENG-TSANG ET AL) 22. August 2000 (2000-08-22) Zusammenfassung Abbildung 3 Anspruch 1 --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
'E' älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
'O' Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
'P' Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
'T' Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
'X' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
'Y' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
'&' Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Juni 2002	27/06/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Sadoune, M-M

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 199 36 939 A (PHILIPS CORP INTELLECTUAL PTY) 6. April 2000 (2000-04-06) Zusammenfassung Anspruch 1 Abbildung 1	1
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 13, 30. November 1999 (1999-11-30) & JP 11 232092 A (NIPPON TELEGR &TELEPH CORP <NTT>), 27. August 1999 (1999-08-27) Zusammenfassung	1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int ales Aktenzeichen
PCT/DE 02/00110

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 0050977	A	31-08-2000	FR	2790347 A1	01-09-2000
			EP	1163562 A1	19-12-2001
			WO	0050977 A1	31-08-2000
US 6108797	A	22-08-2000	TW	408264 B	11-10-2000
DE 19936939	A	06-04-2000	DE	19936939 A1	06-04-2000
			WO	0019386 A1	06-04-2000
			EP	1046142 A1	25-10-2000
JP 11232092	A	27-08-1999	KEINE		